CLAIMS

1. A list signature method comprising at least:

an organizing phase (10) consisting, for a reliable authority (1), of defining parameters for implementing an anonymous electronic signature, including a private key and a corresponding public key,

a phase of registering (20, 20') persons in a list of members authorized to generate an electronic signature specific to the members of the list, during which each person (2) to be registered, calculates (24) a private key (x_i) by means of parameters provided by the reliable authority and by parameters randomly selected by the person to be registered, and the reliable authority delivers (25') to each person to be registered, a certificate ($[A_i, E_i]$) of membership of the list,

a signing phase (30) during which a member of the list generates (35) and issues (36) a signature specific to the members of the list, this signature being built so as to contain proof that the member of the list having issued the signature, has a certificate ($[A_i, E_i]$) of membership of the list, and

a phase of verifying (40) the issued signature, comprising steps (41, 42) for applying a predefined algorithm in order to show proof that the signature was issued by a person having a certificate of membership of the list,

characterized in that it further comprises:

a phase of defining a sequence consisting for the reliable authority (1), of generating a serial number (m) to be used in the signature phase (30), a signature (Sig_{list}) generated during the signature phase comprising a signature element (T_4) which is common to all the signatures issued by a same member of the list with a same serial number and which contains proof that the serial number (m) was used for generating the signature, the verifying phase (40) further comprising a phase for verifying (43) the proof that the serial number (m) was used for generating the signature;

a phase of revoking a member of the list in order to remove a member from the list, during which the reliable authority (1) removes the member to be withdrawn from the list and updates the parameters for implementing the anonymous electronic signature, in order to take into account the removal of the member from the list; and

a phase of updating certificates ($[A_i, e_i]$) of the members of the list in order to take into account changes in the composition of the list.

2. The method according to claim 1, wherein the organizing phase (10) comprises the definition of a common parameter (u) depending on the composition of

the list, the phase for registering (20, 20') a person in the list comprising the definition of a parameter (u_i) specific to the person to be registered which is calculated according to the parameter (u) depending on the composition of the list and which is integrated into the certificate ($[A_i, e_i, u_i]$) handed out to the person, the registering phase (20, 20') comprising a step of updating the common parameter (u) depending on the composition of the list, the phase of revoking a member of the list comprising a step of changing the common parameter (u) depending on the composition of the list, in order to take into account the removal of the member from the list, and the phase of updating certificates of the members of the list including a step for updating the parameter (u_i) specific to each member of the list in order to take into account changes in the composition of the list.

3. The method according to claim 1 or 2, wherein a signature specific to a member of the list and having the certificate $[A_i, E_i]$ comprises parameters T_1, T_2, T_3, such that:

$$T_1 = A_i b^{\omega} \pmod n,$$
$$T_2 = g^{\omega} \pmod n,$$
$$T_3 = g^{e_i} h^{\omega} \pmod n,$$

ω being a number randomly selected during the signing phase (30) and b, g, h and n being general parameters for implementing the group signature, such that parameters b, g and h cannot be inferred from each other by integer power raising modulo n functions, so that the number A_i, and therefore the identity of the member of the list having the certificate $[A_i, e_i]$ cannot be inferred from a signature issued by the member.

4. The method according to any of claims 1 to 3, wherein the number (m) of the series used for generating a list signature is calculated as a function of a date of the beginning of the series.

5. The method according to claim 4, wherein the function for calculating the number of a series is of the form:

$$F(d) = (H(d))^2 \pmod n$$

wherein H is a collision-resistant hash function, d is the date of the beginning of the series, and n is a general parameter for implementing the group signature.

6. The method according to any of claims 1 to 5, wherein a signature (Sig_{list}) issued by a member of the list contains a parameter (T_4) which is calculated

according to the serial number and the private key (x_i) of the signatory member.

7. The method according to claim 6, wherein the parameter T_4 of a signature issued by a member of the list and depending on the serial number m and on the private key x_i of the signatory member is obtained by the following formula:

$$T_4 = m^{x_i} \pmod{n}$$

n being a general parameter for implementing the group signature, and the signature comprises proof that the parameter T_4 was calculated with the private key x_i of the member of the list who issued the signature.

8. An electronic voting method comprising a phase of organizing (50) elections, during which an organizing authority proceeds with generating parameters required for a poll and assigns keys to scrutineers, allowing them to decrypt and verify ballots, a phase for assigning a right of signature to each of the voters, a voting phase (60) during which the voters sign a ballot, and a counting phase (70) during which the scrutineers verify the ballots and calculate the result of the poll according to the contents of the decrypted and valid ballots,
characterized in that it implements a list signature method according to any of claims 1 to 7, for signing the ballots, each voter being registered as a member of a list, and a serial number (m) being generated for the poll, in order to detect whether a same voter has issued several ballots for the poll or not.

9. The voting method according to claim 8, wherein the organizing phase (50) comprises the handing out to each scrutineer of a public key and a private key, the ballots (v_i) are encrypted (62) by means of a public key (Y) obtained by the product of the respective public keys (y_i) of all the scrutineers, and the corresponding decryption private key (X) is obtained by calculating the sum of the respective private keys (x_i) of all the scrutineers.

10. The voting method according to claim 9, wherein encryption (62) of the ballot is carried out by means of a probabilistic encryption algorithm.

11. The voting method according to any of claims 8 to 10, wherein the ballots issued by the votes are stored in a public database (4), in that the result of the verification and counting of each ballot is stored in the database in association with the ballot, and in that the private key (X) for decrypting the ballots is published.